AMENDMENTS TO THE SPECIFICATION

IN THE SPECIFICATION:

Please replace the paragraph beginning on Page 1 Line 9 with the following amended paragraph:

The present invention relates to a digital recording apparatus, a digital ~~recording/reproducing~~ reproducing apparatus, and a digital recording/reproducing apparatus, which record or reproduce video information, audio information and the other data on or from a hard disk, an optical disk or a memory, and an encryption apparatus, a decryption apparatus, an encryption method, and a decryption method.

Please replace the paragraph beginning on Page 3 Line 25 with the following amended paragraph:

Further, the present invention is a digital reproducing apparatus including: a reproducing unit which reproduces a digital recording signal from a recording medium; a data control circuit which controls the reproducing unit and outputs a reproduced digital recording signal; ~~the~~ a memory which is capable of communicating information with the data control circuit; a decryption circuit which is capable of communicating information with the data control circuit, the decryption circuit decrypting the digital recording signal; and a recording signal processing circuit which causes the data control circuit to control

transmission of the digital recording signal. When the digital recording signal encrypted and recorded on the recording medium needs to be decrypted and reproduced, during start-up of the decryption circuit, the digital recording signal having been stored before start-up of the decryption circuit is outputted via the data control circuit. When the decryption circuit is capable of operation, the digital recording signal read by the reproducing unit is transmitted via the data control circuit to the decryption circuit and is decrypted by the decryption circuit to be outputted.

Please replace the paragraph beginning on Page 6 Line 1 with the following amended paragraph:

Moreover, a decryption ~~apparatus~~ method of the present invention includes the steps of: storing a digital signal; decrypting an encrypted digital signal of the digital signal; generating an encryption key for enabling a function of decrypting the digital signal; and determining whether or not the digital signal needs to be decrypted. When the determination is that the digital signal does not need to be decrypted, the digital signal is not decrypted and the stored digital signal is outputted. When the determination is that the digital signal needs to be decrypted, the digital signal from a time of the determination to a time when the function of decrypting is enabled is stored and is decrypted to be outputted after the enabling of the function of decrypting is completed.

Please replace the paragraph beginning on Page 7 Line 11 with the following amended paragraph:

~~FIG. 2 shows~~ FIGs. 2A and 2B show diagrams indicating data transition in a memory in one embodiment of a digital recording apparatus;

Please replace the paragraph beginning on Page 7 Line 16 with the following amended paragraph:

~~FIG. 4 shows~~ FIGs. 4A and 4B show diagrams indicating data transition in a memory in one embodiment of a digital reproducing apparatus;

Please replace the paragraph beginning on Page 7 Line 21 with the following amended paragraph:

~~FIG. 6 shows~~ FIGs. 6A and 6B show diagrams indicating data transition in a memory in one embodiment of a digital recording/reproducing apparatus;

Please replace the paragraph beginning on Page 7 Line 24 with the following amended paragraph:

~~FIG. 7 shows~~ FIGs. 7A and 7B show diagrams indicating data transition in a memory in another embodiment of a digital recording/reproducing apparatus;

Please replace the paragraph beginning on Page 7 Line 27 with the following amended paragraph:

~~FIG. 8 shows~~ FIGs. 8A and 8B show diagrams indicating data transition in a memory in another embodiment of a digital recording apparatus;

Please replace the paragraph beginning on Page 8 Line 3 with the following amended paragraph:

DESCRIPTION OF REFERENCE NUMERALS

1 MPEG encoder, 2a ~~second~~ first data control circuit,

2b second data control circuit,

2c third data control circuit, 3 CPU, 4 memory,

5 encryption circuit, 6 interface,

7 encryption key generation circuit, 8a-8c DVD drive,

9 mutual authentication circuit, 10 decryption circuit, 11 MPEG decoder, 12 selector, 13 selector

Please replace the paragraph beginning on Page 9 Line 20 with the following amended paragraph:

Hereinafter, the generation of the encryption key will be described in detail. In a recording medium such as a DVD disk, the information of the base of an encryption key is recorded in a management information area where management information is recorded. When information to be encrypted is recorded in the recording medium, content information is

encrypted by the use of an encryption key generated from the information of the base of the encryption key recorded in the recording medium and then recorded. Meanwhile, when the encrypted information is reproduced from the recording medium, the encrypted information is decrypted by the use of an encryption key generated from the information of the base of an encryption key recorded in the recording medium and then reproduced. There is a possibility that when the information of the base of an encryption key is read from the recording medium and is passed through the interface 6, the information will be read and deciphered. Therefore, the information of the base of an encryption key is encrypted by an encryption key for key transfer (hereinafter referred to as a "bus key for key transfer") and then transmitted. The bus key for key transfer is generated by the mutual authentication, in which each of the DVD drive 8a and the mutual authentication circuit 9 confirms that the other is a regular device. When a DVD disk is put into the DVD drive 8a, the DVD drive 8a sends a prototype (A) of the bus key that the DVD drive 8a itself has to the mutual authentication circuit 9. The DVD drive 8a and the mutual authentication circuit 9 compute the bus key (A) independently of each other from the prototype (A) of this bus key. The mutual authentication circuit 9 transfers the bus key (A) of computation result to the DVD drive 8a and the DVD drive 8a compares result computed by the DVD drive 8a itself to verify that the same bus keys (A) are generated. Next, a prototype (B) of the bus key that the mutual authentication circuit ~~8~~ 9 itself has is transferred from the mutual authentication circuit ~~8~~ 9 to the DVD drive 8a and then the computation is performed in a similar manner and the mutual authentication circuit ~~8~~ 9 verifies that the bus keys (B) that they mutually compute agree with each other. In this manner, when it is verified that the bus keys (A) agree each other and that the bus keys (B) agree each other, the DVD drive 8a and the mutual

authentication circuit 9 generate the above-mentioned bus keys for key transfer from the bus key (A) and the bus key (B), respectively. Next, to generate an encryption key from the information of the base of an encryption key on the recording medium, the DVD drive 8a encrypts the information of the base of an encryption key on the recording medium by the bus key for key transfer and sends the encrypted information to the mutual authentication circuit 9. The mutual authentication circuit 9 decrypts the received information by the use of the bus key for key transfer to thereby make the information of the base of an encryption key. The key generation circuit 7 generates an encryption key from this information of the base of an encryption key. This encryption key is transmitted to the encryption circuit 5, whereby the encryption circuit 5 is brought to an active state.

Please replace the paragraph beginning on Page 12 Line 1 with the following amended paragraph:

An operation will be described. ~~FIG. 2 shows~~ FIGs. 2A and 2B show diagrams indicating data transition in the memory 4 in one embodiment of a digital recording apparatus according to the present invention. FIG. 2A shows data flowing through the first data control circuit 2a and FIG. 2B shows a change in an amount Sra of data of a recording area in the memory 4 in time series. When a recording medium is put into the apparatus by an operator, the CPU 3 gives the DVD drive 8a a start-up command via the first data control circuit 2a and the interface 6. The DVD drive 8a begins rotating the recording medium and sets various servos and reads information necessary for recording

data on the recording medium. Thereafter, the DVD drive 8a informs the CPU 3 of the completion of preparation via the first data control circuit 2a. Then, when a request of recording a program, copyright of which does not need to be protected by the CGMS is made, the CPU 3 instructs the MPEG encoder 1 to encode a digital recording signal and to input it to the first data control circuit 2a. Each time the MPEG encoder 1 finishes encoding a specified amount of digital recording signals, the MPEG encoder 1 transfers data to an area in the memory 4 assigned for recording via the first data control circuit 2a. This data transfer is finished in a short time because data is transferred between memories at a transfer rate of several hundreds Mbit/sec or more. The data is transferred via the first data control circuit 2a and the interface 6 to the DVD drive 8a and is recorded on the recording medium of the DVD drive 8a. Since a rate at which the DVD drive 8a writes data to the recording medium is approximately several tens Mbit/sec and hence writing data to the recording medium takes several times as long as a period required to transfer data to the memory 4.

Please replace the paragraph beginning on Page 16 Line 17 with the following amended paragraph:

An operation will be described. ~~FIG. 4 indicates~~ FIGs. 4A and 4B indicate diagrams showing the data transition in the memory 4 in one embodiment of the digital reproducing apparatus according to the present invention. FIG. 4A shows data flowing through the second data control circuit 2b in time series and FIG. 4B shows a change in an amount Srb of data of an area in the memory 4 for reading in time series. There will be

described the operation when a digital recording signal that is not encrypted is switched to a digital recording signal that is encrypted while data is being read from the recording medium.

Please replace the paragraph beginning on Page 20 Line 4 with the following amended paragraph:

An operation will be described. ~~FIG. 6 shows~~ FIGs. 6A and 6B show the data transition in the memory 4 in one embodiment of the digital recording/reproducing apparatus according to the present invention. FIG. 6A shows data flowing through the third data control circuit 2c, and FIG. 6B shows a change in an amount Sra of data of an area for recording and a change in an amount Srb of data of an area for reading in the memory 4 in time series.

Please replace the paragraph beginning on Page 22 Line 26 with the following amended paragraph:

An operation will be described. ~~FIG. 7 shows~~ FIGs. 7A and 7B show the data transition in the memory 4 in another embodiment of a digital recording/reproducing apparatus according to the present invention. FIG. 7A shows data flowing through the third data control circuit 2c and FIG. 7B shows a change in an amount Sra of data for recording and a change in an amount Srb of data for reproducing in the memory 4 in time series.

Please replace the paragraph beginning on Page 23 Line 18 with the following amended paragraph:

The flowing of data for recording the video and the reproducing of the video on the display need to be continuously performed even during process of enabling the encryption circuit 5, and hence the writing of the digital recording signal encoded by the MPEG encoder 1 to an area in the memory 4 assigned for recording is continuously performed. Moreover, the data in the area in the memory 4 assigned for reading is continuously supplied to the MPEG decoder 11. When an amount of data in the area assigned for recording is more than a specified amount Sr7 at a time T13 after a time T12b when the enabling of the encryption circuit 5 is completed, the stored data is transferred via the third data control circuit 2c to the encryption circuit 5 and is encrypted by the encryption circuit 5. Further, the data is transferred via the third data control circuit 2c to the memory 4 and is again stored in an area in the memory 4 assigned for writing and then is again transferred via the third data control circuit 2c to the interface 6 and then the writing of the data to the recording medium is started by the DVD drive 8c. The writing of the data to the recording medium is continuously performed until an amount of data for recording decreases to Sr8. Further, when an amount of data in the area assigned for reproducing is less than Sr9, the DVD drive ~~8~~ 8c again starts to read data from the recording medium.

Please replace the paragraph beginning on Page 25 Line 23 with the following amended paragraph:

An operation will be described. ~~FIG. 8 indicates~~ FIGs. 8A and 8B indicate diagrams showing the data transition in a memory in another embodiment of a digital recording apparatus according to the present invention. FIG. 8A shows data flowing through the first data control circuit 2a, and FIG. 8B shows a change in the amount Sra of data of a recording area in the memory 4 in time series.

Please replace the paragraph beginning on Page 27 Line 26 with the following amended paragraph:

The encoded digital recording signal is continuously outputted from the MPEG encoder 1 also after the DVD drive 8a becomes capable of recording data. Since the writing rate of data to the recording medium is faster than the rate of outputting of data by the MPEG encoder 1, the memory 4 does not overflow as shown in FIG. ~~8~~ 8B. The writing of data to the recording medium is not performed until the area in the memory assigned for recording 4 again reaches a specified capacity. Each time the area exceeds a specified capacity, data is written in a lump.

Please replace the paragraph beginning on Page 32 Line 29 with the following amended paragraph:

In the recording side, although information could be transmitted between the third data control circuit 2c and the encryption circuit 5 bidirectionally, information can be transmitted only from the third data control circuit 2c to the encryption circuit 5 in the eighth embodiment. Moreover, both of the third data control circuit 2c and the encryption circuit 5 can transmit information to the selector 12. The selector 12 can select data from the ~~first~~ third control circuit ~~2a~~ 2c or data from the encryption circuit 5 to transmit information to the interface 6.

Please replace the paragraph beginning on Page 33 Line 24 with the following amended paragraph:

Therefore, after data is encrypted by the encryption circuit 5, the encrypted data is not returned via the third data control circuit 2c to an area in the memory 4 assigned for writing. Hence the area in the memory 4 for writing does not need to be secured. Moreover, since an amount of data per unit time passing through the third data control circuit ~~2a~~ 2c becomes smaller, a data transfer rate can be made slower than that in the third and fourth embodiments, which results in reducing the size of the system and further reducing power consumption.